

REMARKS

Claims 1-6 have been rejected under 35 U.S.C. §102(e) as being anticipated by Holloway (US Patent No. 6,424,718 B1). For the reasons that follow, Applicant traverses this ground for rejecting claims 1-6.

The Holloway document and the present application differ materially in the handling of the keys.

In the Holloway disclosure, the private key is encrypted with a key (key encrypting key KEK) and then this block of data is transferred to the client with the applet. This means that the applet should also receive the KEK to be able to retrieve the private key (column 4, lines 50). The KEK extraction is subject to the introduction of a pin code. This has the consequence that the KEK is either the same for all users or unique per user and thus defined when generating the private key.

These Holloway solutions lead to two drawbacks:

- if the KEK is the same for all users, in the case of one user who has retrieved this key while loading his private key, he would be able to extract the private key of another user; and
- if the KEK is unique per user, then at the time of generating the keys pair it is compulsory to assign these keys to a specific user.

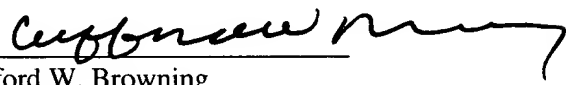
By contrast, in the present application, the private key is encrypted by a service key that never goes out of the server. This private key is at the time of generation not assigned to a specific user. When requested by a user's device, a key pair is selected and associated with the user. The selected private key is decrypted and re-encrypted with a transport key. This transport key, according to the specification, can be a symmetric or

asymmetric key. In the second example, the public key of the security module is described with the meaning that this key is unique for a user.

In order to differentiate more clearly the nature of the keys used by Holloway and in the present invention during the operation of each, Applicant has amended claim 1 to recite that in the present invention the coding of the private key is by means of a secret service key of the generation center, thereby clearly differentiating claim 1 from the Holloway disclosure.

For all these foregoing reasons, Applicant respectfully requests entry of the foregoing amendments, reconsideration of the present application in light thereof and in light of the foregoing remarks, and then allowance of claims 1-6 over all the prior art of record.

Respectfully submitted:

By 
Clifford W. Browning
Reg. No. 32,201
Woodard, Emhardt et al. LLP
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
(317) 634-3456

#354838